AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1.   (Currently Amended) A ~~computer implemented~~ system ~~for~~ that facilitates processing credentials, comprising the following components stored in computer memory and executable by a ~~with~~ processor~~-executable components comprising~~:

   a wrapper that packages credentials associated with resources of a service; and

   a pass-phrase employed in connection with generation of the wrapper *via* a cryptographic wrapping key, the pass-phrase employed to facilitate access to the credentials, the credentials employed to facilitate access to the resources of the service, and the pass-phrase distributed separately from the credentials.

2.   (Canceled)

3.   (Original) The system of claim 1, the credentials providing stronger encryption than the pass-phrase.

4.   (Original) The system of claim 3, the credentials providing greater than 100 bits of encryption.

5.   (Original) The system of claim 3, the pass-phase having human-readable alpha-numeric characteristics.

6.   (Original) The system of claim 1, further comprising one or more partners to request access to the resources.

7.   (Original) The system of claim 6, at least one of the partners includes a credential store to manage the credentials.

8.   (Original) The system of claim 7, the at least one partner distributes the credentials to at least one other partner in order to facilitate access to the resources of the service.

9.   (Original) The system of claim 1, the pass-phase is at least one of spoken, displayed on a screen and typed.

10.   (Original) The system of claim 1, further comprising at least one of a Secure Socket Layer (SSL), a Virtual Private Network (VPN), and a dedicated line to establish connections to the service.

11.   (Original) The system of claim 10, further comprising a remote login utilizing a basic authentication over the SSL.

12.   (Original) The system of claim 10, further comprising at least one SSL certificate to establish connections to the service.

13.   (Original) The system of claim 1, the services are associated with a platform provisioning service.

14.   (Original) The system of claim 13, the platform provisioning service associated with at least one partner, the partner including at least one of a tenant and a service provider to form at least one of a billing, a financial, and an accounting service.

15.   (Original) The system of claim 14, the partner employs the pass-phrase to unlock the credentials and achieve access to the platform provisioning services.

16.   (Original) The system of claim 14, at least one of the platform provisioning service and the partner maintain an account to process the credentials, the at least one of the platform provisioning service and the partner employ a Universal Resource Locator (URL) to present the credentials to the account.

17.   (Original) A computer-readable medium having computer-executable instructions stored thereon to perform at least one of processing and the generation of the wrapper and the pass-phrase of claim 1.

18.   (Currently Amended) A method to facilitate a security connection between entities, comprising:

       generating a strong password;

       generating a pass-phrase;

       wrapping the password cryptographically *via* the pass-phrase, wherein the pass-phrase facilitates in unlocking the wrapper;

       storing the wrapped password in an executable; and

       transmitting the executable and the pass-phrase to a system *via* different communications mediums.

19.   (Canceled)

20.   (Previously Presented) The method of claim 18, further comprising employing the pass-phrase to unlock the strong password stored in the executable, the strong password employed to establish a trust relationship with an entity.

21.   (Original) The method of claim 18, further comprising at least one of:

       requesting a Secure Sockets Layer (SSL) connection; and

       presenting an SSL certificate in response to the request.

22.   (Original) The method of claim 21, further comprising at least one of:

       verifying an SSL certificate;

       requesting a Universal Resource Locator (URL) from a listener;

       presenting authentication credentials to a receiver; and

       logging in a caller to an account.

23.   (Original) The method of claim 18, further comprising limiting access to the executable.

24.   (Original) The method of claim 18, further comprising at least one of:

      setting up account privileges;

      designating account contacts; and

      verifying the contacts.

25.   (Original) The method of claim 24, further comprising verbally communicating the pass-phrase.

26.   (Original) The method of claim 25, further comprising transmitting and storing the password and the pass-phrase separately.

27.   (Currently Amended) A computer executable system to facilitate a security relationship between parties, comprising:

      means for generating a password;

      means for generating a pass-phrase;

      means for generating a package of credentials, wherein the credentials are packaged by wrapping them cryptographically;

      means for storing the password separate from the package;

      means for locking the package with the pass-phrase; and

      means for transmitting the package and the pass-phrase to a system *via* different communications mediums.

28.   (Currently Amended) A computer-readable medium having stored thereon a ~~signal~~ data structure to communicate security data between at least two nodes, comprising:

      a first data packet comprising:

      an encapsulated password component employed to establish a trust relationship between at least two nodes, wherein a wrapper field is employed to encapsulate the password, the wrapper field mediating access to the password; and

      a second data packet comprising:

      a pass-phrase employed to generate and unlock the wrapper field, the pass-phrase distributed separately from the wrapper field.

29.   (Original) The signal of claim 28, wrapper field being cryptographically weaker than the password.

30.   (Canceled)

31.   (Currently Amended) A ~~computer implemented~~ system to establish a trust relationship, comprising the following ~~computer executable~~ components stored in computer memory and executable by a processor:

        a service that controls one or more resources, the service issues credentials to facilitate access to the resources;

        a wrapper generated by the service to package the credentials; and

        a pass-phrase employed to generate the wrapper and mediate access to the service, the pass-phrase distributed separately from the credentials.

32.   (Original) The system of claim 31, the service is a provisioning service that establishes a trust relationship between one or more partners *via* the credentials.

33.   (Cancelled)